aurigin

Document Summary


New Search


Help

Preview Claims
Preview Full Text
Preview Full Image

Email Link: 

Document ID:	JP 2000-089666 A2
Title:	ENCODING/DECODING DEVICE
Assignee:	NIPPON TELEGR & TELEPH CORP
Inventor:	SUGITA MAKOTO
US Class:	
Int'l Class:	G09C 1/00 A; H04L 9/06 B
Issue Date:	03/31/2000
Filing Date:	09/16/1998

Abstract:

PROBLEM TO BE SOLVED: To achieve an encoding/decoding device capable of ensuring guarantee of higher safety than a conventional one.

SOLUTION: In an encoding/decoding device which encodes and decodes data at every block of a constant bit length by plural steps of encoding processing using a common secret key to the decoding and encoding, an encoding function part for realizing an encoding function is configured of non-linear processing parts 301-1-301-4 executing the disturbing calculations by using a common key created from a secret key for an inputted data and outputting the calculation results, and linear processing parts 302-1-302-3 inputting the data outputted from the non-linear processing parts and executing predetermined linear calculations and outputting the calculation results, with the 4 steps of the non-linear processing parts and the 3 steps of the linear processing parts alternately cascaded.

(C)2000,JPO

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－89666
（P2000－89666A）
(43)公開日　平成12年３月31日(2000.3.31)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０９Ｃ　1/00	６１０	Ｇ０９Ｃ　1/00	６１０Ａ	５Ｊ１０４
Ｈ０４Ｌ　9/06		Ｈ０４Ｌ　9/00	６１１Ａ	

審査請求　未請求　請求項の数１　ＯＬ　（全７頁）

(21)出願番号　特願平10－262073

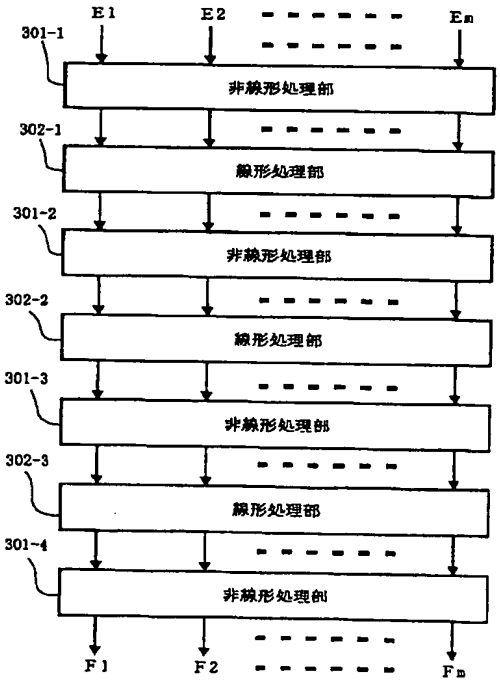
(22)出願日　平成10年９月16日(1998.9.16)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　杉田　誠
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100064908
弁理士　志賀　正武

Ｆターム(参考)　5J104 AA01 JA10 NA08

(54)【発明の名称】　暗号化／復号化装置

(57)【要約】
【課題】従来に比べより高い安全性の保証が可能な暗号化／復号化装置を実現する。
【解決手段】復号化および暗号化に共通の秘密鍵を用い、複数段の暗号化処理段によって、一定のビット長のブロック毎にデータの暗号化および復号化を行う暗号化／復号化装置において、複数段の暗号化処理段において暗号化関数を実現する暗号化関数部が、入力されたデータに対して秘密鍵から生成された鍵を用いて攪乱演算を行って演算結果を出力する非線形処理部３０１－１～３０１－４と、非線形処理部から出力されたデータを入力し、所定の線形演算を行って演算結果を出力する線形処理部３０２－１～３０２－３とを、交互に、非線形処理部を４段と、線形処理部を３段、縦段接続して構成されている。



1

【特許請求の範囲】
【請求項１】　復号化および暗号化に共通の秘密鍵を用い、一定のビット長のブロック毎にデータの暗号化および復号化を行う暗号化／復号化装置において、
各段の入力データの半分のビット数を有する第１のデータを所定の暗号化処理を行う暗号化関数部に入力して得られる該暗号化関数部の出力を入力データの他の半分のビット数を有する第２のデータにビット毎にＸＯＲして得られる第３のデータと、第１のデータとを出力する暗号化処理段を、互いに複数段接続し、該複数段の暗号化処理段によって暗号化／復号化処理を複数回繰り返し行うことでデータの暗号化又は復号化を行うものであって、
前記暗号化関数部が、
入力されたデータに対して秘密鍵から生成された鍵を用いて攪乱演算を行って演算結果を出力する非線形処理部と、
非線形処理部から出力されたデータを入力し、所定の線形演算を行って演算結果を出力する線形処理部とを、
交互に、非線形処理部を４段と、線形処理部を３段、縦段接続してなることを特徴とする暗号化／復号化装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は共通鍵暗号アルゴリズムにおけるブロック暗号方式を用いた暗号化／復号化装置に係り、特に、差分解読法や線形解読法に対して強い暗号化／復号化装置に関する。
【０００２】
【従来の技術】図１に、暗号化および復号化において共通の秘密鍵を用いる共通鍵暗号の一方式であるデータの暗号化および復号化を一定のまとまった長さ毎に行うブロック暗号方式による暗号化および復号化装置（以下、暗号化／復号化装置）の基本的な機能構成を示す。図１に示す暗号化／復号化装置は、ｊ個のそれぞれ暗号化／復号化処理を行う暗号化処理段１０１－１，１０１－２，…，１０１－ｊから構成されている。この暗号化／復号化装置は、６４ビット、１２８ビット等の一定のブロック長毎に平文Ｓ又は暗号文Ｔを入力して、複数の暗号化処理段１０１－１，１０１－２，…，１０１－ｊによって暗号化又は復号化処理を複数回繰り返し行い、それぞれ入力文と同一のブロック長を有する暗号文Ｕ又は平文Ｖを出力する。各暗号化処理段１０１－１，１０１－２，…，１０１－ｊでは暗号化／復号化処理の際に、秘密鍵のデータに基づく計算処理が行われる。その際、各暗号化処理段１０１－１，１０１－２，…，１０１－ｊでは、１つの複数ビットの秘密鍵からビット単位の転置、シフト等により生成された異なる複数の鍵が使用される。なお、暗号化と復号化の処理では、各暗号化処理段１０１－１，１０１－２，…，１０１－ｊで用いられる複数の鍵の使用順序が互いに逆順となる。また、以下

2

の説明では暗号化と復号化で共通する事項に対して、暗号化に関連する名称、用語を代表して使用する。
【０００３】図２は、図１における暗号化処理段１０１－１～１０１－ｊの各段における機能構成を示すブロック図である。図２に示す暗号化処理段は、２つの入力に対してビット毎に排他的論理和を行って出力する排他的論理和回路（以下、ＸＯＲ回路）２０１－ｉと、複数ビットからなる鍵を用いた暗号化処理を行う暗号化関数部２０２－ｉから構成されている。入力Ｓ、あるいは前段から出力されたデータのブロック長の左半分のビットのＰｉ－１は、ＸＯＲ回路２０１－ｉへと入力され、暗号化関数部２０２－ｉの出力Ｒｉとビット毎に排他的論理和（以下、ＸＯＲ）が行われて、後段の右半分の入力となる出力Ｑｉ（＝Ｐｉ－１（＋）Ｒｉ）として出力される（（＋）はＸＯＲを示す）。一方、各段の入力データの右半分のビットのＱｉ－１は、暗号化関数部２０２－ｉへ入力されるとともに、後段の左半分の入力となる出力Ｐｉ（＝Ｑｉ－１）として出力される。ここでｉは図１の暗号化処理段の段数に対応する１～ｊの整数であり、Ｐ０およびＱ０は入力データＳ又はＴに、Ｐｊ＋１およびＱｊ＋１は出力データＵ又はＶに対応するデータである。
【０００４】図２に示す暗号化関数部２０２－ｉの従来の構成の一例を図７に示す。図７は、共通鍵暗号として広く使用されている「ＤＥＳ暗号」（Data Encryption Standard；米国ＮＩＳＴ（National Institute of Standards and Technology）の規格）（以下、従来技術１と称する）における暗号化関数部の構成を示すブロック図である。図７に示す暗号化関数部２０２－ｉでは、入力された３２ビットのＱｉ－１が拡大転置部８０１で所定の転置表（変換表）を用いた拡大転置によって４８ビットのデータに変換されてＸＯＲ回路８０２へと入力される。ＸＯＲ回路８０２は６４ビットの秘密鍵からあらかじめ生成されていたｉ段用の４８ビットの鍵と拡大転置部８０１の出力とでＸＯＲを行って４８ビットのデータを出力する。ＸＯＲ回路８０２の出力は各６ビットずつに分けられ、８個のＳボックスと呼ばれるデータ置換部（Ｓ１～Ｓ８）８０３－１～８０３－８へと入力される。各Ｓボックス８０３－１～８０３－８では、入力された各６ビットのデータに対して所定の置換表に基づくデータの置き換えが行われて各４ビットのデータが出力される。さらに転置部８０４で所定の転置表に基づいてビット位置の転置が行われて３２ビットの処理結果Ｒｉが求められる。
【０００５】なお、「ＤＥＳ暗号」では、図１に示す暗号化／復号化装置の暗号化／復号化の処理は１６回の繰り返しである。また、暗号化／復号化装置の全体の構成としては、図１の構成に対して、入力段と出力段に、それぞれ初期転置処理と逆初期転置処理を行うブロックが追加されている。また、各暗号化処理段では、１つの６

3

４ビットの秘密鍵から生成されたそれぞれ異なる１６個の４８ビットの鍵が使用されるようになっている。

【０００６】図８に、図２に示す暗号化関数部２０２－ｉの他の従来の構成例を示す。図８は、ＮＴＴ（日本電信電話株式会社）によって開発された１２８ビットブロックアルゴリズムを採用した「Ｅ２」という共通鍵暗号アルゴリズム（以下、従来技術２と称する）における暗号化関数部の構成を示すブロック図である。図８に示す暗号化関数部２０２－ｉでは、入力された６４ビットのデータＱｉ－１が各８ビットのデータｘ１，ｘ２，…，ｘ８に分割された後、非線形処理部９０１へ入力される。非線形処理部９０１では、入力されたデータｘ１，ｘ２，…，ｘ８が、８個のＸＯＲ回路によって１２８ビットの秘密鍵から生成された第１の鍵Ｋ（１）とＸＯＲされて、その演算の結果が８個のＳボックスへそれぞれ入力される。８個のＳボックスでは、予め定められた置換表を参照することで入力データに対して置換処理が行われ、各８ビットのデータｚ１，ｚ２，…，ｚ８が出力される。ここで、非線形処理部９０１では、Ｓボックスというデータ置換部において置換処理を行うことで、出力として、入力データに対して非線形な変換処理を行ったデータが得られることになる。

【０００７】非線形処理部９０１から出力されたデータｚ１，ｚ２，…，ｚ８に対しては、データ変換層９０２において下式で示す線形演算処理が行われる。

【数１】

4

$$\begin{pmatrix} z'_1 \\ z'_2 \\ z'_3 \\ z'_4 \\ z'_5 \\ z'_6 \\ z'_7 \\ z'_8 \end{pmatrix} = P \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \\ z_7 \\ z_8 \end{pmatrix}$$

ここで行列Ｐは

$$P = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

【０００８】なお、図８に示すデータ変換層９０２は、１６個のＸＯＲ回路から構成されているが、これは上式を実現する一例であって、内部の構成については限定されない。

【０００９】データ変換層９０２から出力された各８ビットのデータｚ１'，ｚ２'，…，ｚ８'は、非線形処理部９０３へ入力される。非線形処理部９０３では、非線形処理部９０１と同様にして、８個のＸＯＲ回路を用いて入力データｚ１'，ｚ２'，…，ｚ８'と秘密鍵から生成された第２の鍵Ｋ（２）とでＸＯＲを行い、さらに８個のＳボックスで予め定めた置換表を参照することで置換処理を行い、処理結果として各８ビットのデータｙ１，ｙ２，…，ｙ８を出力する。

【００１０】非線形処理部９０３から出力された各８ビットのデータｙ１，ｙ２，…，ｙ８には、さらに８ビットを単位とする左回転処理が行われる。そして回転処理の結果が暗号化関数の処理結果Ｒｉとして出力される。

【００１１】なお、アルゴリズム「Ｅ２」では、図１に示す暗号化／復号化装置が１２段の暗号化／復号化処理段を有して構成されている。暗号化／復号化装置の全体の構成としては、図１の構成に対して、入力段と出力段に、それぞれ初期変換処理と最終変換処理を行うブロックが追加されている。また、各暗号化処理段では１つの

5

１２８ビットまたは１９２ビットもしくは２５６ビットの秘密鍵から生成されたそれぞれ異なる１２個の鍵が使用され、初期変換処理と最終変換処理の各ブロックでは各２個の異なる鍵が使用されるようになっている。

【００１２】以上の説明したように、従来技術１においては、図７に示すように各暗号化関数部においてＳボックスを用いる非線形な処理を行うデータ置換部が１段設けられ、さらにこの暗号化関数部を有する暗号化処理段を複数段設けることによって安全性の向上が図られている。従来技術２では、図８に示すように暗号化関数において、Ｓボックスを用いる非線形処理部で置換されたデータを線形処理部で変換し、さらに、もう一度Ｓボックスを用いる非線形処理部でデータを置換することにより、さらなる安全性の向上を図っている。

【００１３】

【発明が解決しようとする課題】しかしながら上記従来の装置は、最大平均差分確率という暗号化の強度評価（最悪値が１、最良値がp^{27}、ｐは０以上１以下の値）として最も一般的な尺度において、従来技術１の場合で１、従来技術２の場合でp^{12}であり、何れの場合もこの尺度における理論的最大値であるp^{27}に比べて低い安全性しか保証できないという課題があった。

【００１４】この発明の目的は、従来技術に比べより高い安全性の保証が可能な暗号化／復号化装置を実現することにある。

【００１５】

【課題を解決するための手段】上記課題を解決するため、請求項１記載の発明は、復号化および暗号化に共通の秘密鍵を用い、一定のビット長のブロック毎にデータの暗号化および復号化を行う暗号化／復号化装置において、各段の入力データの半分のビット数を有する第１のデータを所定の暗号化処理を行う暗号化関数部に入力して得られる該暗号化関数部の出力を入力データの他の半分のビット数を有する第２のデータにビット毎にＸＯＲして得られる第３のデータと、第１のデータとを出力する暗号化処理段を、互いに複数段接続し、該複数段の暗号化処理段によって暗号化／復号化処理を複数回繰り返し行うことでデータの暗号化又は復号化を行うものであって、前記暗号化関数部が、入力されたデータに対して秘密鍵から生成された鍵を用いて撹乱演算を行って演算結果を出力する非線形処理部と、非線形処理部から出力されたデータを入力し、所定の線形演算を行って演算結果を出力する線形処理部とを、交互に、非線形処理部を４段と、線形処理部を３段、縦段接続してなることを特徴としている。

【００１６】この発明によれば暗号化／復号化装置の何れにおいても、暗号化関数部において非線形処理部と線形処理部が交互にそれぞれ４段、３段多段縦段接続された暗号化関数を用いることにより、暗号化関数の最大平均差分確率を小さくすることによって全体としての安全性を高めることができる。

6

【００１７】

【発明の実施の形態】以下、図１～図６を参照して本発明の実施形態について説明する。本発明による暗号化／復号化装置全体としての基本的な構成は、従来の例として説明した「ＤＥＳ」や「Ｅ２」のような他のブロック暗号化方式による構成と同様に、図１に示す構造を有している。すなわち本発明による暗号化／復号化装置は、図１に示すように暗号化処理段１０１－１～１０１－ｊが多段縦段接続された構成を有している。図１では、その多段縦段の初段のデータとして各ｂビットのブロック長を有する平文Ｓ又は暗号文Ｔが入力され、終段の出力として各ｂビットのブロック長を有する暗号文Ｕ又は平文Ｖが出力される。

【００１８】次に、図１における各暗号化処理段１０１－１～１０１－ｊとしては、従来の技術と同様に図２に示すような構成を用いることができる。各暗号化処理段１０１－ｉ（ｉは１～ｊ）には、図２に示すようにブロック長（ｂビット）をそれぞれ半分に分割したデータＰｉ－１とデータＱｉ－１を入力し、データＱｉ－１を暗号化関数部２０２－ｉに入力して得られる出力Ｒｉを、ＸＯＲ回路２０１－ｉによってデータＰｉ－１にビット毎（bit-wise）のＸＯＲして得られるＰｉ－１（＋）Ｒｉ（（＋）はＸＯＲを表す）を次段の入力Ｑｉとする。また、Ｑｉ－１をそのまま次段の入力Ｐｉとして出力するような構造を考える。

【００１９】次に、本発明が特徴とする構成である図２に示す暗号化関数部２０２－ｉの構成について説明する。本発明においては、暗号化関数部２０２－ｉを、図３に示すように、非線形処理部３０１－１，３０１－２，３０１－３，および３０１－４と線形処理部３０２－１，３０２－２，および３０２－３が交互にそれぞれ４段と、３段縦段接続された構造とする。非線形処理部３０１－１，３０１－２，３０１－３，および３０１－４と、線形処理部３０２－１，３０２－２，および３０２－３では、それぞれ入力された平文Ｓ又は暗号文Ｔのブロック長ｂビットの半分のビットをｍ分割した値（ｍは２以上、ｂの半分以下の整数）と等しいビット数（ｎビットとする）を有するｍ個のデータが並列に入出力される。図３では、入力段となる非線形処理部３０１－１の入力データをＥ１，Ｅ２，…，Ｅｍ、出力段となる非線形処理部３０１－４の出力データをＦ１，Ｆ２，…，Ｆｍとしている。

【００２０】図３に示す各非線形処理部３０１－１～３０１－４は、それぞれ図４に示すように各ｎビットのデータＣ１，Ｃ２，Ｃ３，…，Ｃｍと、各ｋビットの鍵Ｋ１，Ｋ１，…，Ｋｍとを入力して置換演算を用いた撹乱演算を行って各ｎビットのデータＤ１，Ｄ２，Ｄ３，…，Ｄｍを出力するｍ個の演算部４０１－１～４０１－ｍから構成されている。これらｍ個の演算部４０１－１

～４０１－ｍは、並列して動作する。各ｋビットの鍵Ｋ１，Ｋ１，…，Ｋｍは、従来の場合と同様にして１つの秘密鍵から置換、ビットシフト等の処理によって予め生成しておく。なお、非線形処理部において用いる鍵Ｋ１，Ｋ２，…，Ｋｍは、図１の各暗号化処理段１０１－１～１０１－ｊ毎に異なる値とすることが望ましい。また、各暗号化処理段内で、あるいは各非線形処理部内で、鍵Ｋ１，Ｋ２，…，Ｋｍを同一の値にすることも可能である。

【００２１】図５は、図４に示す非線形処理部の内部構成のより具体的な構成を示すブロック図である。図５に示す非線形処理部は、各ｎビットの入力Ｃ１，Ｃ２，…，Ｃｍをそれぞれ入力して、入力データと同じビット長の各ｎビットの鍵Ｋ１，Ｋ２，…，Ｋｍとビット毎のＸＯＲをとるＸＯＲ回路５０１－１，５０１－２，…，５０１－ｍと、各ＸＯＲ回路５０１－１，５０１－２，…，５０１－ｍの出力に対して、所定の置換表による置換処理を行うことでデータに対して撹乱演算を行う置換部５０２－１，５０２－２，…，５０２－ｍから構成されている。置換部５０２－１，５０２－２，…，５０２－ｍは、図７～図８を参照して説明した従来の構成におけるＳボックスと同様の構成を用いることができる。置換部５０２－１，５０２－２，…，５０２－ｍからは、それぞれｎビットのデータＤ１，Ｄ２，…，Ｄｍが出力されて、後続する線形処置部へと入力されるか、または最最終段であれば暗号化関数部の出力となる。

【００２２】図６に図３に示す線形処理部３０２－１～３０２－３の具体的構成を示す。図６においては行列Ａの値を例えば下式のように予め定め、各線形処理部３０２－１～３０２－３の入力となる各ｎビットのデータＧ１，Ｇ２，…，Ｇｍに線形作用させる線形変換を定めている。図６に示す構成では、入力データＧ１～Ｇｍと、行列Ａから、各ｎビットの出力Ｈ１，Ｈ２，…，Ｈｍを下式のようにして求める。ただし、下式は、平文Ｓ又は暗号化文Ｔのブロック長を１２８ビット、ブロックの分割数ｍを８、各データＧ１，Ｇ２，…，ＧｍおよびＨ１，Ｈ２，…，Ｈｍのビット数を８ビットとする場合の例である。

【数２】

$$\begin{pmatrix} H_1 \\ H_2 \\ H_3 \\ \bullet \\ \bullet \\ \bullet \\ \bullet \\ Hm \end{pmatrix} = A \begin{pmatrix} G_1 \\ G_2 \\ G_3 \\ \bullet \\ \bullet \\ \bullet \\ \bullet \\ Gm \end{pmatrix}$$

ここで行列Ａは

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

【００２３】なお、本発明による暗号化／復号化装置は、論理回路によるハードウェアによって実現することもできるし、計算機とその計算機で実行される暗号化／復号化プログラムとの組み合わせによって実現することも可能である。また、暗号化／復号化プログラムは、計算機読み取り可能な記録媒体に記録して、あるいはネットワークを介して頒布することが可能である。

【００２４】

【実施例】上記発明の実施の形態において最大平均差分確率という安全性評価尺度においてｊ＝８の場合に実際に計算することにより各置換の最大平均差分確率をｐと定めたとき、暗号化関数部が$2p^8$という理論的最良値（p^8）に近い値を示し、暗号全体として$8p^{24}$という高い安全性が保証可能であることが確認された。これは従来技術１、２の場合と比べて高い安全性が保証可能であることを示している。

【００２５】

【発明の効果】本発明によれば、４段の非線形処理部と３段の線形処理部を交互に接続してなる暗号化関数部を用いて暗号化処理手段を構成することによって、従来技術に比べ非常に高い安全性の保証が可能な暗号化／復号化装置を実現することが可能になる。

【図面の簡単な説明】

【図１】　ブロック暗号化方式による暗号化／復号化装置の機能構成を示すブロック図である。

【図２】　図１における暗号化処理段の機能構成を示すブロック図である。

【図３】　本発明が特徴とする図２における暗号化関数部の機能構成を示すブロック図である。

【図４】　図３における非線形処理部の機能構成を示すブロック図である。

【図５】　図４における非線形処理部の具体的な構成を示すブロック図である。

【図６】　図３における線形処理部の具体的構成を示す＊ブロック図である。

【図７】　従来技術１における暗号化関数部の機能構成を示すブロック図である。

【図８】　従来技術２における暗号化関数部の機能構成を示すブロック図である。

【符号の説明】

１０１－１～１０１－ｊ　暗号化処理段

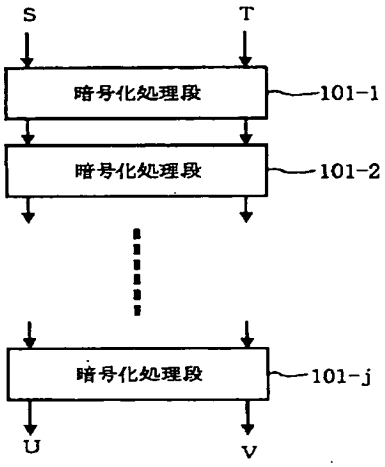
２０１－ｉ　ＸＯＲ回路

２０２－ｉ　暗号化関数部

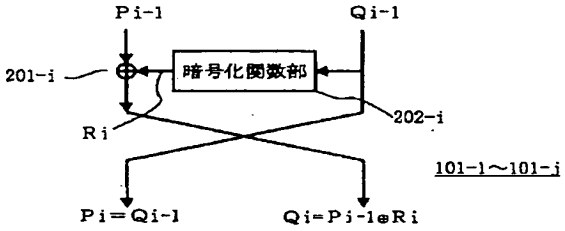
３０１－１～３０１－４　非線形処理部

３０２－１～３０２－３　線形処理部

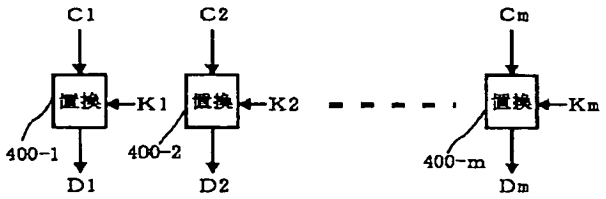
【図１】



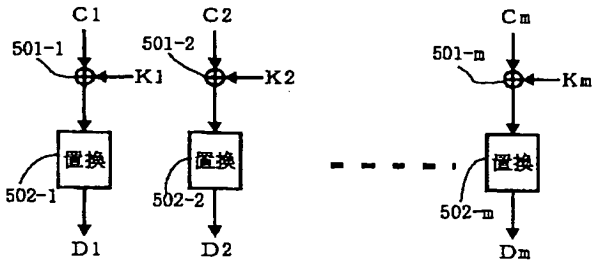
【図２】



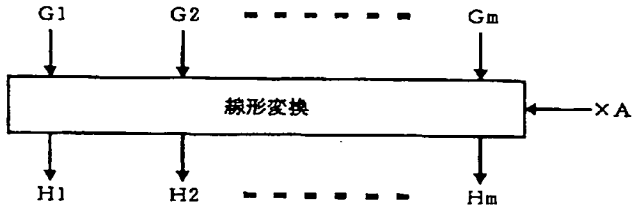
【図４】



【図５】

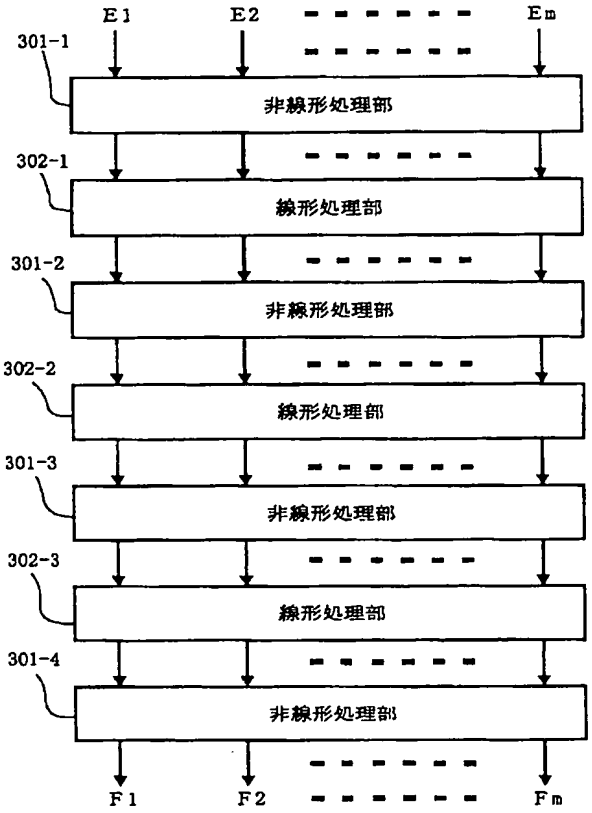


【図６】

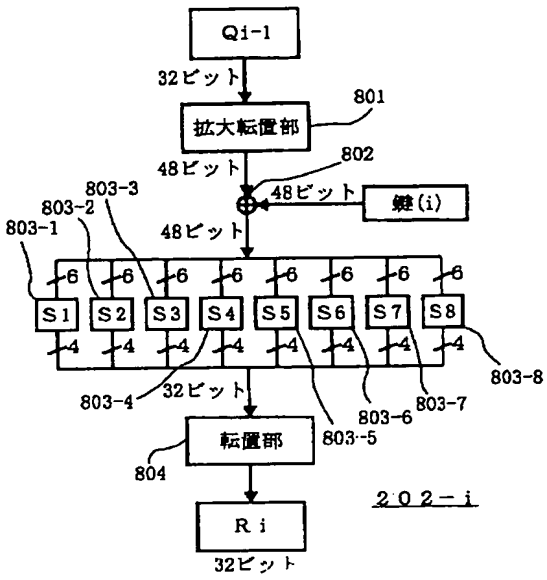


$$A=\begin{bmatrix} 0,1,1,1,1,1,1,0 \\ 1,0,1,1,0,1,1,1 \\ 1,1,0,1,1,0,1,1 \\ 1,1,1,0,1,1,0,1 \\ 1,1,0,1,1,1,0,0 \\ 1,1,1,0,0,1,1,0 \\ 0,1,1,1,0,0,1,1 \\ 1,0,1,1,1,0,0,1 \end{bmatrix}$$

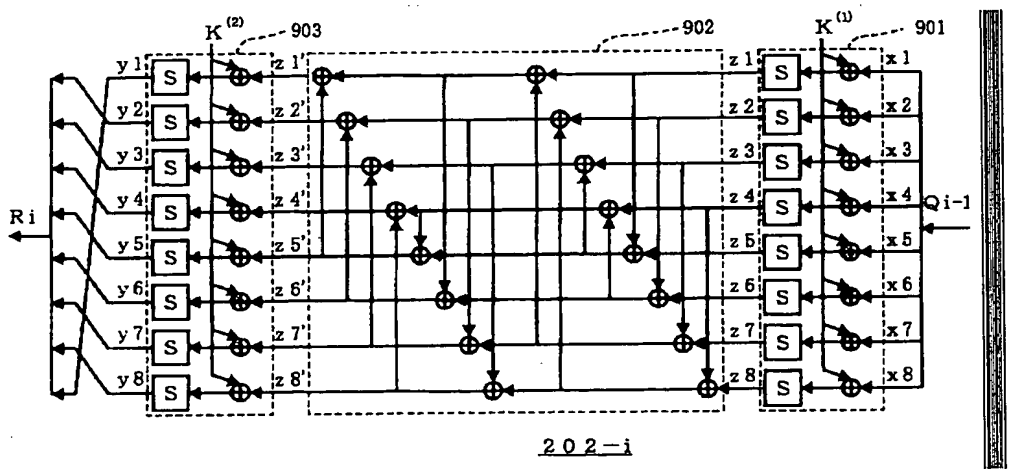
【図３】


E1
E2
Em
301-1
非線形処理部
302-1
線形処理部
301-2
非線形処理部
302-2
線形処理部
301-3
非線形処理部
302-3
線形処理部
301-4
非線形処理部
F1
F2
Fm

【図７】


Qi-1
32ビット
拡大転置部
801
48ビット
802
48ビット
鍵(i)
803-3
803-2
803-1
48ビット
6
S1
S2
S3
S4
S5
S6
S7
S8
4
803-8
803-4
32ビット
803-6
803-7
803-5
転置部
804
２０２－ｉ
Ri
32ビット

【図８】


K(2)
903
902
K(1)
901
y1
y2
y3
y4
y5
y6
y7
y8
S
z1'
z2'
z3'
z4'
z5'
z6'
z7'
z8'
z1
z2
z3
z4
z5
z6
z7
z8
x1
x2
x3
x4
x5
x6
x7
x8
Ri
Qi-1
２０２－ｉ